

GAO

Report to the Subcommittee on
Personnel, Committee on Armed
Services, U.S. Senate

January 1999

DEFENSE IRM

Alternatives Should Be Considered in Developing the New Civilian Personnel System



19990202 013

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

Accounting and Information
Management Division

B-278058

January 27, 1999

The Honorable Wayne Allard
Chairman
The Honorable Max Cleland
Ranking Minority Member
Subcommittee on Personnel
Committee on Armed Services
United States Senate

During the past 5 years, the Department of Defense (DOD) has been reducing the costs associated with civilian personnel management by reducing the number of staff working in personnel, consolidating selected personnel management functions at newly created regional centers, and attempting to improve personnel management business processes. A key part of this initiative is Defense's development of a new information management system—the Defense Civilian Personnel Data System (DCPDS)—to support a wide range of personnel management functions including recruitment, staffing, benefits administration, and training. Defense expects to complete deployment of this system by March 2000. This letter responds to the request from your subcommittee that we answer the following questions about this initiative and recommend corrective actions, where appropriate.

- *How did Defense determine the number and locations for civilian personnel regional service centers and why is there a wide disparity in the number of regional centers among the services?*
- *In overseeing, managing, and developing DCPDS, is Defense applying the investment principles of the Clinger-Cohen Act?*
- *Does DCPDS duplicate a system that is available through the Office of Personnel Management (OPM) called the Employee Express System?*
- *Was Defense leadership aware of the extent and cost of the needed modifications to the commercial-off-the-shelf (COTS) software application?*
- *Has Defense identified and mitigated the risks associated with the major COTS modifications?*

In conducting our review, we examined Defense requirements on development, management, and oversight of information systems in light of relevant legislative and federal requirements, including the Clinger-Cohen Act of 1996. We discussed Defense's efforts to develop and manage DCPDS with officials from (1) Defense's Civilian Personnel

Management Service (CPMS), (2) the Air Force Central Design Activity (CDA) responsible for managing technical modifications, (3) Oracle Corporation, the contractor from which Defense acquired the new system, (4) the military services and Defense agencies that plan to use the system, and (5) the Office of Personnel Management. We also visited and interviewed officials from five of the regional personnel centers and four of the local or installation-level offices. We conducted our review from August 1997 through October 1998 in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the Department of Defense. The Acting Assistant Secretary for Force Management Policy provided us with written comments. These comments have been incorporated where appropriate and are discussed in the Agency Comment and Our Evaluation section of this letter and appendix I. Details on the scope and methodology of our work are provided in appendix II.

Results in Brief

Defense's current initiative can potentially improve civilian personnel operations and achieve cost savings. However, because the Department has not examined other business process alternatives that could potentially achieve even greater savings and process efficiencies, there is no assurance that this is the best alternative for civilian personnel operations.

Before embarking on its costly initiative to improve personnel management, Defense examined two alternatives (1) outsourcing personnel computer operations to the Department of Agriculture's (USDA) National Finance Center¹ and (2) regionalizing personnel centers. It determined that it would take the National Finance Center about 6 years to prepare for transferring computer operations and that some new functionality built into its legacy system would be lost.

However, Defense did not examine several other potentially effective alternatives, including (1) continuing to centralize all or parts of its personnel management operations to reduce duplicative layers of oversight at the components and ensure more consistent operations DOD-wide, (2) integrating its personnel and payroll management systems, (3) restructuring its regional offices to serve multiple components rather than perpetuating regional offices dedicated to only one component, (4) restructuring local personnel offices to serve multiple bases or

¹The National Finance Center provides payroll, personnel, financial, and other administrative services to USDA agencies as well as a broad range of federal departments and agencies.

installations (they now serve only one base or installation), and (5) outsourcing all civilian personnel operations to the private sector.

These alternatives are feasible and may have helped Defense to achieve even greater savings and efficiencies than the current approach. For example, as of June 1998, there were 886 people performing civilian personnel management and oversight functions at component headquarters and major command levels at a cost of about \$63 million annually. By consolidating some or portions of these component oversight functions, Defense could reduce the number of staff that perform duplicative overhead functions and decrease personnel management oversight costs. In addition, the Defense Science Board² determined that integrating payroll and personnel systems was a viable and cost beneficial option for military personnel. Among other benefits, this alternative might have enabled the Department to cut system operation and maintenance costs as well as streamline and dramatically improve both payroll and personnel business processes. Furthermore, by having regions serve multiple services and agencies, Defense could have further consolidated regional offices and reduced duplicative regional overhead costs. The Washington Headquarters Service has already demonstrated the feasibility of this option by managing personnel services for numerous smaller Defense agencies.

CPMS officials who were responsible for the personnel initiative said that they did not consider these business processing alternatives because (1) CPMS did not have authority to require the military services and Defense agencies to adopt such approaches, (2) the Department did not allow sufficient time to rigorously examine alternatives, and (3) the Department lacked basic cost and performance data needed to study the alternatives. As a result, Defense selected a business processing alternative which, in the long run, may not provide the most effective personnel operations at the lowest cost.

In addition, after it decided on its approach, Defense did not follow a sound process for selecting regions. For example, it did not require military services and Defense agencies to base their decisions on data-driven analyses and it allowed only a short time frame for the selection. Consequently, the analyses of the services and agencies were inconsistent, considering different factors in choosing their regions, and none included a formal cost/benefit analysis. As a result, there is a wide

²Report of the Defense Science Board Task Force: Military Personnel Information Management, August 31, 1996.

disparity in the numbers of regions selected, and there is no convincing rationale or objective evidence that any of the selections were optimal.

Furthermore, Defense did not adequately consider a full range of technical options before deciding to replace its legacy system with the Oracle COTS product. Defense informally surveyed the potential market of COTS³ products and selected three COTS packages for further evaluation. It then considered functional, technical, and cost differences among the three but did not rigorously analyze their costs, benefits, and expected returns-on-investment nor did it assess the desirability of continuing to use the legacy system. After the Oracle product was acquired, Defense performed a limited economic analysis for the system which did not consider all of the promising business operation options or all of the technical options and did not separate the costs and benefits of the selected regionalization approach from those of the Oracle product. As a result, there is still no objective evidence that either element of Defense's approach (regionalization or the use of the Oracle product) is the best option.

Finally, after Defense acquired the Oracle system, it did not mitigate critical technical risks, as the following examples illustrate.

- Because the Oracle product did not satisfy many federal and Defense-unique requirements, modifying the system would entail a significant effort. Further, there was no guarantee that the modifications would be successful or that the system would be able to accommodate Defense's large-scale workload. To mitigate this risk, Defense could have first worked with the developer to define unique Defense and federal personnel requirements and postponed purchasing the product until after it was modified. While Defense worked with the developer to define unique Defense and federal requirements, it committed to purchasing the product before the software was modified and could be demonstrated to perform successfully.
- Defense has not fully mitigated critical security risks for either the legacy- or the Oracle-based systems. Despite the fact that these systems contain sensitive privacy data, Defense has not established encryption or firewall standards.⁴ These standards are needed to ensure a consistent level of protection for personnel data and to ensure that all DCPDS partners can

³Over 100 different software products were initially identified.

⁴Encryption involves the transformation of original text (also known as plaintext or cleartext) into unintelligible text (also known as ciphertext). Firewalls are hardware and software components that check all incoming network traffic and block unauthorized traffic.

safely and effectively access the system. In addition, Defense has not promoted security awareness among the local offices that will be operating the new system.

- Defense has not adequately addressed risks associated with the Year 2000 computing problem. While it has made good progress in renovating the legacy system and ensuring the modern system's compliance, it has not developed agreements with its data exchange partners that specify date format changes, time frames for these changes, or processes for resolving interface conflicts. In addition, Defense has not developed adequate contingency plans for either of the systems. Even if systems are compliant, civilian personnel business operations are at risk of disruptions caused by external interfacing systems and the public infrastructure. As such, detailed contingency plans are necessary to ensure that Defense can maintain the basic functionality of its core civilian personnel operations.

Background

Defense's civilian personnel community provides Defense managers with the personnel management services and support needed to accomplish their missions, including recruitment, job classification, position management, training, career development, and benefits administration. Traditionally, the military services and Defense agencies have managed their civilian personnel service delivery organizations and systems through local civilian personnel offices located at or near military bases and installations all over the world. During the past 5 years, Defense has been attempting to reduce personnel management costs through the following actions.

(1) *Reducing the number of civilian personnelists.* Personnelists provide face-to-face assistance to civilian employees, answering questions about such issues as life insurance, health insurance, and position classification. They process paperwork for new hires, promotions, awards, and a wide variety of personnel actions and assist in training, benefits administration, management/employee relations, recruitment, and staffing. In 1994, Defense reported that a single personnelist served about 67 employees. Defense's goal was to reduce the number of personnel staff to the point where one personnelist served 88 employees by the year 2001 and 100 employees by the year 2003.⁵ As of June 30, 1998, Defense reported that it

⁵In 1989, the Army and the Air Force had civilian personnelist servicing ratios of 1 to 50 and 1 to 48, respectively, while the Navy's ratio was 1 to 61. At the time, DOD began efforts to increase servicing ratios in the other services to at least the Navy's ratio. The goal of reaching 1:100 was derived based on recommendations by the National Performance Review, as well as DOD's own internal benchmarking study. DOD's internal study indicated that some DOD organizations had servicing ratios exceeding 1:100.

had cut 1,700 personnelists and had achieved a ratio of 1 personnelist to 77 employees.

(2) *Improving personnel management processes.* To help increase the personnelist-to-civilian employee ratio, Defense is attempting to improve and automate its personnel management business processes. For example, it has automated and improved processes for (1) developing, tracking, and monitoring all personnel actions, (2) handling injury compensation claims, and (3) estimating retirement eligibility and benefits. It has acquired an automated tool called RESUMIX, which helps personnelists analyze resumes of people applying for a position with Defense. It is also developing an interactive voice response system that enables employees to use a Touch-Tone phone to change selected data in their own personnel records.

(3) *Creating regional centers.* Defense is creating regional centers that will specialize in selected personnel management functions and reducing the number and size of local offices. It anticipates that specialization of labor within the regions combined with improved business processes will reduce operating costs. As of September 30, 1998, the Army had established all 10 of its planned regions, the Navy had established 7 of 8 planned regions, the Air Force had established its 1 region, and the Defense agencies participating in this initiative had established all 3 of their planned regions. Table 1 further illustrates the changes in personnel management that will occur through Defense's improvement initiative.

Table 1: Differences in Personnel Management

Before personnel improvements	After personnel improvements
Local personnel offices provided service to all civilian employees and carried out all work processes, such as processing paperwork for new hires, processing promotions, developing vacancy announcements, and assisting in management/employee relations.	Local personnel offices will still provide face-to-face service to civilian employees. However, 40 to 60 percent of the processing of personnel-related actions are to be done at the regional offices.
Some personnelists specialized in certain work processes while others provided a broader range of personnel services.	Most personnelists at the local offices will be generalists. Specialists will be located at regions.
In 1994, there were 389 local offices and no regional offices.	By fiscal year 1999, there are to be 311 local offices plus 22 regional offices.
Most work processes were manual and paper-oriented.	Business process improvement efforts are targeted at automating many work processes, such as estimating retirement eligibility and benefits and analyzing resumes.
Before 1994, only personnelists had access to personnel management systems.	Functional managers, civilian employees and personnelists are to have access to the personnel management information system. Among other things, civilians can view their own records and make prescribed changes to insurance and thrift savings retirement data. Functional managers will be able to initiate personnel actions on the system.

A COTS Personnel Management System Is Acquired to Support Initiative

At the beginning of this effort, Defense components operated a number of personnel management information systems that assisted in all aspects of personnel operations, such as developing position classification documents; preparing vacancy announcements; and processing appointments, reinstatements, transfers, promotions, retirements, and terminations. These systems were redundant and not interoperable, and Defense believed that they were antiquated.

To modernize this environment, Defense eliminated the duplicative systems and used the Air Force civilian personnel management information system, located in San Antonio, Texas, to do all personnel processing. This legacy system meets Defense-unique personnel management requirements; is able to process Defense's large-scale workload successfully; and because it operates in one location, it can be maintained by CDA personnel with experience in operating and protecting systems. However, Defense believed that there were a number of

significant shortfalls with this mainframe system⁶ and, therefore, the system should be replaced with a new COTS system. For example, according to Defense

- the legacy system relied on outdated technology for its database structure, file update, and retrieval;
- manpower resources and costs needed to develop and maintain the system were extensive;
- the system required duplicative data entry;
- the system could only be accessed by personnelists—it could not be easily modified to provide access to civilian employees so that they could review and make prescribed changes to their own benefit, insurance, and other personnel-related data;
- modifications reflecting improvements in business processes were difficult to make; and
- the system was not Year 2000 compliant.

As a result, Defense acquired a COTS product from Oracle Corporation. In contrast to the legacy system, which operated on two 1970s era mainframes, the new system will operate in a distributed, networked environment⁷ at regional and local offices. According to Defense, the system

- will enable any authorized civilian employee with a personal computer to directly access the system and to perform prescribed personnel-related operations or management tasks,
- can be easily modified to reflect improvements in business processes,
- will cost less to maintain and operate, and
- will be Year 2000 compliant.

However, because the Oracle product was originally designed for use in the private sector, it did not satisfy all federal and Defense-unique requirements for personnel management. For example, it could not process federal personnel forms, such as the standard personnel action form (Form 52). It did not address the federal General Schedule for salaries, Defense's demonstration projects for pay banding, or the Defense-unique salary schedule for tens of thousands of foreign nationals who work for the Department overseas but do not get the same salaries or

⁶A mainframe is a very large computer capable of supporting hundreds or even thousands of users simultaneously. Mainframes use smaller computers as front-end processors that connect to communications networks.

⁷Rather than processing all applications on a single mainframe, applications are distributed to run on independent, networked computers.

benefits as American employees. It did not have DOD-unique data for security and mobilization. In addition, it did not directly interface with Defense's existing payroll system. As a result, the product needed to be modified and/or enhanced before it was deployed.

The Civilian Personnel Management Service (CPMS), which was established in 1993 to provide departmentwide leadership for the civilian personnel business area, is responsible for managing the new system. CPMS acquired the system using an indefinite delivery, indefinite quantity (IDIQ) DOD contract⁸ under which Oracle Corporation was a participating vendor. Defense components are responsible for purchasing and maintaining hardware to support the new system. CPMS has assigned the Air Force Central Design Activity (CDA) responsibility for managing technical modifications to the system under the contract.⁹ According to CPMS, the system is currently in the test phase. Once system qualification tests are completed, the system will be deployed to four test sites during January and February 1999. The Air Force Operational Test and Evaluation Center (AFOTEC) will then evaluate the test results to ensure that the system meets user needs in an operational environment. Deployment to the remaining sites is expected to begin in late 1999 and end by March 2000. DOD officials stated that this schedule is likely to slip at least 2 months to ensure that the system is fully tested and meets user needs before it is fully deployed.

Costs of DOD's Personnel Initiative

The cost of Defense's personnel initiative is estimated to be \$1.2 billion over its estimated 15-year life cycle (fiscal years 1995 through 2009), of which Defense reports that over \$300 million has been spent through the end of fiscal year 1998. These totals are itemized in table 2.

⁸The Integrated Computer-Aided Software Engineering (I-CASE) contract. This is an indefinite delivery, indefinite quantity contract awarded to Logicon in April 1994. DOD can use this contract to purchase IT systems, hardware, and software tools from approved vendors without having to prepare a separate contract.

⁹There is an integrated team of contractors working for CDA in San Antonio that includes Oracle staff as well as individuals who work on a contract basis for CDA. The Oracle employees work on Oracle's federal system while the other contract employees are responsible for developing DOD-unique add-ons to the system.

Table 2: Estimated Costs of Defense's Personnel Initiative (Dollars in Millions)

Purpose	Estimated cost	Amount spent through fiscal year 1998
Cost to develop and deploy the new system.	\$177	\$142
Cost to establish regional offices.	\$190	\$159
Operational and support costs for the new system for fiscal years 1999 through 2009. ^a	\$621	\$0
Operational and support costs for regions for fiscal years 1995 through 2009. ^a	\$256	\$13
Total	\$1,244	\$314

^aThis includes costs for site operations, replacement software and hardware, equipment upgrades, program management oversight, and administration.

Question: How Did Defense Determine the Number and Locations for Regional Centers and Why Is There a Wide Disparity?

Answer: Defense considered only a narrow range of alternatives for improving personnel operations before deciding to regionalize personnel centers. This left the Department without assurance that it was pursuing the most cost-effective and beneficial approach. After it decided to regionalize, Defense did not follow a sound process for selecting regions, it did not require services and agencies to base their decisions on data-driven analyses. Consequently, the analyses of the services and agencies were inconsistent, each considering different factors in choosing regions and none included a formal cost/benefit analysis. This process resulted in the wide disparity in the number of regions chosen, and it left Defense without the objective data needed to determine whether any of the choices were optimal.

Before embarking on a major, costly initiative to improve personnel management, sound practices call for examining a range of improvement options, including those that would radically change the current way of doing business. For example, in addition to, or instead of regionalizing, Defense could have considered (1) outsourcing its personnelist computer operations or all of its civilian personnel management services, (2) integrating its personnel/payroll management systems, (3) creating regions that cross-service between agencies and the military services, (4) consolidating local personnel offices that are near each other to provide face-to-face services to multiple bases or installations out of the same office, and/or (5) centralizing all, or portions of, civilian personnel management in DOD. By thoroughly considering these and other choices, Defense would have ensured that the most cost-effective and beneficial

alternative was chosen before deciding to invest \$367 million¹⁰ in the project and that any systems acquired or developed would support the most efficient and effective business processes.

Defense did not examine all of these promising alternatives. Instead, it considered only the possibility of outsourcing computer operations with the National Finance Center. This option was determined to be infeasible.¹¹ Defense did not analyze other alternatives, including cross-servicing, integrating payroll/personnel systems, collocating personnel offices, DOD-wide management of personnel operations, or outsourcing all of its personnel operations.

In addition, once it decided on regionalization, Defense did not follow a sound process for selecting the regions. For example, Defense did not require the services and agencies to base their selections on data-driven analyses. In fact, the services were allowed to select whichever and as many regions as they wanted as long as they achieved at least a 1 to 88 personnelist-to-civilian employee ratio.

Consequently, the services considered different factors in choosing their regions. However, none based their selections on a thorough cost/benefit analysis. This resulted in the wide disparity in the number of regions chosen, as the following examples illustrate.

- The Army and the Navy considered the distance between regions, proximity to the installations they serviced, and coverage across time zones as well as some costs associated with establishing and operating regions and transferring personnel. After considering these factors, the Army selected 10 regions and the Navy selected 8. It was decided that the regions would be responsible for about 60 percent of the work while local offices would be responsible for about 40 percent. Neither the Army or the Navy conducted cost/benefit analyses in making their decisions. Nor did they consider the costs of personnel work processes or the relationship between per capita servicing costs and region size.
- Because it had already demonstrated that it could reduce overhead and technology costs and facilitate standardization in service and business

¹⁰Defense planned to initially invest \$177 million to develop and deploy the new system and \$190 million to establish the regional offices, for a total of \$367 million.

¹¹Defense considered the possibility of outsourcing the IRM support function to the private sector. It concluded that this option was not feasible due to the size of Defense's operations. In exploring the possibility of outsourcing computer operations with the National Finance Center, Defense learned that it would take the Center about 6 years to prepare for transfer and that some new functionality built into its legacy system would be lost.

processes by collocating the civilian personnel center with its military center, the Air Force decided to use a single Air Force personnel center to serve all of its personnel. The Air Force decided that its local offices would continue to be responsible for about 53 percent of the work.

While Defense allowed the services wide latitude in choosing their regions, it directed that its agencies be serviced by three regional offices.¹² The two largest agencies—the Defense Finance and Accounting Service and the Defense Logistics Agency—were directed to establish their own regions and the Washington Headquarters Service was directed to serve as a regional personnel office for the smaller agencies. The Defense Finance and Accounting Service selected the location for its regional center based on the fact that it had already started to regionalize personnel operations there. The Defense Logistics Agency selected the location for its regional center after considering the location and space availability of its depots. However, neither conducted formal cost/benefit analyses in choosing their regions or considered the cost of personnel work processes and the relationship between per capita servicing costs and region size.

CPMS officials cited several reasons for taking this approach. First, they pointed out that CPMS had no authority to require the services and agencies to base their decisions on thorough, data-driven analyses or, in fact, to require that they adopt any standard personnel system or approach at all. At the same time, they noted that the military services had a vested interest in maintaining the status quo and had the independent budget authority to see that the status quo was preserved. Second, Defense lacked basic cost and performance data for examining options, including data on the cost of personnel work processes and the relationship between per capita servicing costs and region size. Third, the agency was directed in 1994 to implement the Office of the Secretary of Defense's (OSD) recommendations quickly, i.e., to reduce the number of personnelists to a ratio of one personnelist to every 88 civilian employees by fiscal year 1998. CPMS officials held that this did not allow time to develop objective data and rigorously examine alternatives. The 1 to 88 goal was later extended to the year 2001. Fourth, CPMS officials stated that because most of the costs for performing personnel functions are for personnelists, and systems, facilities, and operations constitute relatively smaller costs, as long as it

¹²DOD has over 20 separate agencies and activities. Most are small and in the Washington, D.C. area. The intelligence agencies were excluded from this initiative and allowed to acquire their own personnel software program (PeopleSoft).

achieved the 1 to 88 ratio, Defense would accrue significant cost savings regardless of the number of regions selected.¹³

Nevertheless, several of the alternatives Defense ignored offered the opportunity to achieve far greater savings while streamlining personnel operations, as the following examples illustrate.

- By consolidating some or all of its personnel management, Defense could reduce the numbers of staff that perform duplicative overhead functions. As of June 1998, there were 886 people performing civilian personnel management and oversight functions at component headquarters and major command levels at a cost of about \$63 million annually.¹⁴ Furthermore, if Defense had centralized management of departmentwide personnel operations, it could take a departmentwide perspective in deciding which local offices and which regions should be consolidated.
- Cross-servicing could have enabled Defense to further consolidate regional offices and reduce duplicative overhead costs. Some Defense components have already found this alternative to be beneficial. The military services, for example, are doing some cross-servicing with employees in remote locations and the Washington Headquarters Service is servicing the smaller Defense agencies as well as some federal agencies, including the Office of Personnel Management.¹⁵ Additionally, having local personnel offices service multiple bases or installations could further reduce duplicative overhead costs.
- Integrating payroll and personnel systems could have helped Defense reduce system operation and maintenance costs as well as further streamline and improve personnel and payroll management business processes. In fact, after considering the potential benefits of this alternative and its feasibility, the Defense Science Board recommended it as a solution for military personnel in 1996.¹⁶

While it may have required more time and greater management commitment to change Defense practices, the potential for substantially greater savings and efficiencies should have compelled Defense to

¹³According to Defense's economic analysis, over 80 percent of the costs of performing personnelists functions are for personnelists.

¹⁴Our estimate is based on DOD/CPMS data on personnelists costs and numbers.

¹⁵Defense does not have information on the savings being derived from its current cross-servicing activities.

¹⁶Report of the Defense Science Board Task Force: Military Personnel Information Management, August 31, 1996.

perform a rigorous analysis of all alternatives and to select the one proven most cost effective.

Question: In Developing, Managing, and Overseeing DCPDS, Is Defense Applying the Clinger-Cohen Act?

Answer: Defense did not adequately apply the three requirements of the Clinger-Cohen Act of 1996 we reviewed which are designed to maximize the value of major investments. While the act was passed after Defense initiated its development of DCPDS, the act's requirements reflect basic and widely accepted principles of sound system acquisition management. Similar practices are also called for by Defense's own system acquisition regulations and guidelines, Office of Management and Budget (OMB) guidance, and other legislative requirements effective at the time DCPDS decisions were made, including the Government Performance and Results Act of 1993, the Federal Acquisition Streamlining Act of 1994, the Paperwork Reduction Act of 1995, and the Chief Financial Officers Act of 1990.

The Clinger-Cohen Act requires federal agencies to focus on the results achieved through information technology investments while streamlining the federal information technology (IT) procurement process. Specifically, this act introduces much more rigor and structure into how agencies approach the selection and management of IT projects. Although the act was passed after Defense decided to develop a new personnel management system, its principles are based on practices that are widely considered to be integral to successful IT investments.¹⁷

We examined whether Defense applied the following three requirements of Clinger-Cohen, which are designed to maximize the value of a major investment such as DCPDS.

(1) Agency heads should analyze the missions of the agency and, based on the analysis, revise the agency's mission-related and administrative processes, as appropriate, before making significant investments in IT supporting those missions.

(2) Investments should be selected based on objective data, including quantitatively expressed projected net, risk-adjusted return on investment,

¹⁷See Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994) for an analysis of the management practices of several leading private and public sector organizations on which the Clinger-Cohen Act is based and Assessing Risk and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making (GAO/AIMD-10.1.13, February 1997) for an overview of the IT management process envisioned by the Clinger-Cohen Act.

and specific quantitative and qualitative criteria for comparing and prioritizing alternative information system projects.

(3) Agency heads should ensure, through the use of performance measurements, that mission-related benefits are defined and assessed for all IT investments.

Defense Did Not Reengineer Business Processes Before Investing in DCPDS

Defense did not reengineer its personnel processes before investing in the new system. Before initiating development, CPMS and the individual services conducted an extensive effort to identify and document the preproject business processes at the local offices. Most of the improvements they made to these operations were minor. For example, they developed automated tools to help personnelists analyze resumes and to track civilian employee costs. However, for the most part, these initiatives did not involve radical or major changes to existing processes. As noted in the previous section, Defense considered only the option for outsourcing computer operations and failed to consider other alternatives that had the potential to provide significantly greater benefits, such as integrating personnel and payroll systems, centralizing personnel management, or cross-servicing. Because Defense did not examine these options, there is no evidence that the personnel management system acquired will support the most effective way of doing business or provide optimal return on investment.

Costs, Benefits, and Returns on Investments Not Adequately Analyzed

Costs, benefits, and returns on investments were not adequately analyzed before Defense acquired the Oracle package. Defense informally surveyed the potential market of COTS products and selected products from PeopleSoft, Inc., Integral Software Systems, Inc., and Oracle Corporation for evaluation. In evaluating these products, a DOD team considered various characteristics of the software products, including functionality, technical merit, and cost.

However, Defense did not perform a rigorous analysis of costs, benefits, and returns on investments for these products before deciding to acquire the Oracle product, nor did it rigorously analyze the other available commercial products or the possibility of continuing to use the legacy system. The importance of developing complete and accurate analyses of the costs/benefits and returns of system alternatives is underscored by several governmentwide requirements in addition to the Clinger-Cohen Act. For example, OMB's Circular A-130, Management of Federal

Information Resources, calls on agencies "to conduct benefit-cost analyses to support ongoing management oversight processes that maximize return on investment and minimize financial and operating risks for investments in major information systems and on an agencywide basis." Likewise, Supplement to OMB's Circular A-11 (July 1997), Part 3, Capital Programming Guide Version 1.0, and OMB Bulletin No. 95-03, Planning and Budgeting for the Acquisition of Fixed Assets, state that "the planning for fixed asset acquisitions should be based on a systematic analysis of expected benefits and costs." Because Defense did not perform these analyses, it does not know if it chose the best system.

Once an alternative is selected, Defense regulations¹⁸ require that an economic analysis be prepared to compare the selection against the status quo. This analysis establishes baseline life cycle costs, estimates benefits for the new system, and calculates expected return on investment. However, Defense did not perform an economic analysis before acquiring the new system. In addition, the analysis that Defense performed after the initiative was underway did not separate the costs and benefits of the system from costs and benefits associated with cutting personnel and regionalizing. As a result, Defense still does not know if it chose the best business process alternative.

Performance Measures Developed but Data Needed for Comparisons Is Lacking

To measure how the Oracle product supports its personnel administration mission, CPMS developed four major mission performance measure categories to be collected by each service and Defense agency. These categories included (1) servicing ratio, (2) customer satisfaction, (3) process cycle time (e.g., how long it takes to process a specific personnel action, such as filling an opening or promoting an employee), and (4) regulatory compliance (i.e., whether personnel paperwork complies with applicable laws and regulations). The military services and Defense agencies then developed several detailed measures within the categories, and CDA and CPMS developed several information technology or system-level measures to measure DCPDS' contribution to the mission area, including process cycle time and system response time.

However, because military services have not agreed on two fundamental definitions, they will not be able to calculate these measures consistently and compare measures across services. First, the military services could not agree on how to define the start and end date for the process of filling

¹⁸Economic analyses are required by DOD's Instruction 7041.3, "Economic Analysis for Decisionmaking" and its "5000" acquisition regulations.

a position or whether certain personnel actions (rejecting a list of qualified job applicants, for example) would be considered as part of the process for filling a position. Second, they could not agree on a common definition of "paperwork errors." Because the military services are not using common definitions, some critical performance measures will not be comparable across DOD. In addition, Defense does not have baseline performance information on how long it takes to fill a position and the accuracy of personnel paperwork. As a result, it will not be able to accurately assess whether the system has improved mission performance in these areas or by how much.

Question: Does DCPDS Duplicate Employee Express?

Answer: DCPDS is not a duplicate of OPM's Employee Express system. OPM's Employee Express system is designed to be used in conjunction with existing personnel and payroll systems of the agencies. It does not perform all basic personnel and payroll functions. Instead, it allows employees to interface with the existing personnel and payroll systems. For example, Employee Express enables a federal civilian employee to use a Touch-Tone phone or personal computer connected to the Internet to make changes to certain data in his/her automated personnel/payroll records.¹⁹

The new DCPDS system is to eventually replace existing DOD personnel systems. It is intended to support the full range of core functional requirements needed by Defense for an automated human resources management system, including position management and classification, recruitment and staffing, personnel action administration, benefits administration, labor-management and employee relations, work force development, and retention and reporting. These requirements are defined in a November 1997 study by the Human Resources Technology Council, an inter-agency group associated with the President's Management Council and chaired by the Office of Personnel Management. Although Defense civilian employees will not be able to use the Employee Express system to make changes to DCPDS data, Defense plans to add employee express-type features at a later date that will allow changes to be made using a Touch-Tone phone or personal computer connected to the Internet.

¹⁹For example, direct deposit information, financial allotments, federal and state tax withholding, home or check mailing address, health benefits, and Thrift Savings Plan contributions.

Question: Was Defense Leadership Aware of Extent and Cost of Modifications?

Answer: Defense leadership was aware that the COTS package it acquired would need to be substantially modified in order to support federal and Defense-unique personnel requirements although the full extent of the modification was not known. According to the Acquisition Program Manager, Oracle had orally agreed not to charge Defense for the modifications it was making to the system because it believed it could market the package to other federal agencies after it was "federalized."

Question: Has Defense Identified and Mitigated Risks Associated With the COTS Modifications?

Answer: Defense has not identified and mitigated significant risks associated with its acquisition. Specifically, as discussed below, Defense does not yet know (1) if the modifications will satisfy DOD needs and provide required functionality and performance, (2) how it will handle future system modification, (3) how it will maintain the system, (4) how it will protect sensitive data in the system, and (5) how it will ensure the continuity of core civilian personnel operations in the event of Year 2000 failures.

Defense Does Not Know If Modifications Will Satisfy Requirements

Defense has no assurance that the modified product being developed by Oracle will meet all its needs. It does not know whether Oracle can provide all required functionality and performance or deliver it on time. Although Defense worked closely with Oracle to define requirements and test the changes that were made to the COTS package, it acquired the system before these modifications were completed and before the modified product could be tested. As a result, Defense faces the risk that the system it has already acquired may not meet all its requirements. This risk could have been avoided by waiting for Oracle to produce the "federalized" product and thoroughly testing it before purchasing it.

Defense Does Not Know How It Will Handle Future System Modification

Compounding the risk that the system will not meet Defense requirements is the fact that Defense has not secured the legal right to modify and upgrade the package it has acquired. CPMS obtained a software licensing agreement for 3 years (with an option to extend to 8 years) that provides for Oracle to correct programming errors found in its product. However, the agreement does not require Oracle to provide upgrades to DOD's modified product at the same time and at the same cost as it provides upgrades to its private sector commercial product. As a result, Defense has no assurance that Oracle will make future versions of the software available to Defense at a reasonable cost or make future needed modifications at a reasonable cost, so that its version of Oracle product

will not become obsolete. In addition, the agreement does not specify whether Oracle will make DOD-required modifications to its customized product, or how much Oracle will charge for such work.

DOD Does Not Know How It Will Maintain the System

CPMS has not taken several actions which are essential to ensuring that the system is adequately maintained. First, CPMS has not yet developed agreements between the DCPDS partners that define each partner's responsibility for systems, operations, maintenance, and security. Whereas the legacy system was centrally maintained, the military services and Defense agencies will be responsible for maintaining the new system hardware and related local area networks. It is critical that CPMS develop agreements with its DCPDS partners to ensure effective, efficient, and secure systems operations and maintenance.

Second, CPMS has not yet established a configuration control board comprised of DCPDS users to assist in deciding what changes need to be made to the system once it is deployed and to prioritize change requests. As noted in Defense's Program Manager's Guide to Software Acquisition Best Practices, configuration management is vital to the success of any software effort because it prevents uncontrolled, uncoordinated changes to shared project software and products (documentation and test results, for example).

Third, CPMS has not decided who will provide technical assistance to the personnel sites operating the system. CDA currently performs this function; however, CPMS has not decided whether to continue using CDA after deployment or to outsource this function.

Fourth, CPMS has not yet developed agreements with DCPDS interface partners, which include the Office of Personnel Management and DOD agencies responsible for payroll, security, and manpower systems. As noted in Defense's Program Manager's Guide to Software Acquisition Best Practices, interfaces constitute essential elements of the system but are not completely controlled by the developer. As a result, the guide recommends that explicit written agreements with interface partners be developed to ensure that the partners clearly understand their roles and responsibilities.

Defense Has Not Adequately Addressed Security Risks

It is even more difficult to protect the new system and its data than it is to protect the legacy system and its data. Whereas the mainframe-based legacy system operated in one location and was maintained by CDA

personnel with experience in protecting information systems, the new system will be distributed to 22 centers and many local offices where staff have little or no experience in providing the type of security required for DCPDS. Furthermore, both systems are vulnerable to outside computer attacks since they use an unsecure telecommunications network to transmit data.²⁰

According to our Executive Guide: Information Security Management,²¹ there are five key principles for managing these types of risks that were identified by studying private and government organizations with reputations for having good information security programs. First, organizations should assess their risks and determine their security needs. Second, they should establish a central management focal point for security issues. Third, they should implement appropriate policies and related controls. Fourth, they should promote security awareness. Fifth, they should continually monitor and evaluate policy and control effectiveness. An important factor in effectively implementing these principles is linking them in a cycle of activity that helps ensure that information security policies address current risks on an ongoing basis.

A security risk assessment was performed for the new system, a central security focal point was established, and some effective measures were implemented, including a software application that can identify and notify appropriate officials of unauthorized or suspicious attempts to access personnel data and produce summary audit reports highlighting unauthorized access attempts. However, Defense has not implemented appropriate departmentwide or DCPDS-specific security policies and related controls nor effectively promoted security awareness as indicated by the following examples of identified weaknesses which have increased both the legacy and modern system's vulnerability to computer attacks.

- Defense officials, including the Deputy Secretary of Defense, believe that encryption technology is necessary to maintain the secrecy and integrity of data that is transmitted over Defense's unsecure networks. Encryption involves the transformation of original text (also known as plaintext or cleartext) into unintelligible text (also known as ciphertext). However, the Defense Information Systems Agency (DISA), which is responsible for establishing computer security standards for the Department, has not established a standard encryption approach for sensitive but unclassified Defense data. In the absence of these standards, CPMS is planning to

²⁰Defense uses its Non-Secure Internet Protocol Router Network (NIPRNet) to transmit DCPDS data.

²¹Executive Guide: Information Security Management (GAO/AIMD-98-68, May 1998).

acquire a package for encrypting DCPDS data. As other organizations do the same, DOD may be faced with managing multiple, incompatible encryption products and approaches.

- The military services and Defense agencies recognize that firewalls, which are hardware and software components that check all incoming network traffic and block unauthorized traffic, are also essential to protecting sensitive data and have begun installing them. However, DISA has not established standards to ensure a consistent level of protection and to ensure that computer systems protected by firewalls can still communicate with each other.
- During our review, we identified several sites that were not maintaining adequate physical security over computer resources, indicating a lack of security awareness at the local level. For example, at two of the four local personnel offices we visited, the door to the computer room was unlocked. At one of these offices, one of the computer room's walls consisted of a row of standard metal filing cabinets, offering little obstruction to the room even if the door had been locked. At a third local office, the computer room was collocated with the office's paper shredder, to which the personnel office staff were given unsupervised access. Also, the network communications room at one of the local offices was unlocked and personnel office staff were given unsupervised access to the room. Additionally, at one of the four regional offices we visited, the network communications room door was unlocked and tied open. Further, our review identified fire protection deficiencies at four offices—three local offices and one regional office. Specifically, the four offices did not have automatic fire detection equipment in or near the computer room.
- Our review identified problems with disaster recovery procedures and planning for the regional and local offices. For example, we observed inadequate data backup and recovery procedures at one of the four regions visited. In this regard, the draft DCPDS Trusted Facilities Manual, dated February 2, 1998, noted that Defense had not resolved basic disaster recovery planning issues for DCPDS such as, "what data to backup, how often that data will require backup, the method of backup, and testing to ensure the backup has been accomplished successfully."²² Additionally, the military services had not completed service-level or site-specific disaster recovery plans for their regional and local personnel offices. As of July 1998, CDA had drafted guidelines for the services and agencies to use in developing disaster recovery plans, but it did not have complete data on the number of regional and local offices that had finalized and tested site-level disaster recovery plans. After discussions on this issue, CDA

²²Final draft of the Trusted Facilities Manual dated February 2, 1998, Section 6.5, Trusted Backup and Recovery Guidance.

began requiring all sites to provide these plans before becoming operational. However, neither CPMS nor CDA have determined how the plans will be tested or whether CDA will periodically verify that the disaster recovery plans are updated.

Year 2000 Risks Not Fully Mitigated

The Year 2000 computing problem is rooted in the way dates are recorded and computed in automated information systems. For the past several decades, systems have typically used two digits to represent the year, such as "97" to represent 1997, in order to conserve electronic data storage and reduce operating costs. With this two-digit format, however, the Year 2000 is indistinguishable from 1900, or 2001 from 1901, etc. As we reported earlier this year, the impact of computer failures resulting from the problem could be widespread, costly, and potentially disruptive to military operations.²³ Year 2000 problems could adversely affect Defense's ability to train civilian personnel, administer benefits, recruit staff, and handle management/employee disputes. However, Defense has not fully mitigated this risk.

We compared Defense's efforts to correct the Year 2000 problem to criteria detailed in our Year 2000 Assessment Guide.²⁴ This guide advocates a structured approach to planning and managing an effective Year 2000 program through five phases: (1) raising awareness of the problem, (2) assessing the extent and severity of the problem and identifying and prioritizing remediation efforts, (3) renovating, retiring, or replacing systems, (4) validating or testing corrections, and (5) implementing corrected systems. We and OMB established a schedule for completing each of the five phases, including requiring agencies to complete the assessment phase by August 1997 and the renovation phase by September 1998.

Our Assessment Guide also identifies other dimensions to solving the Year 2000 problem, such as identifying interfaces with outside organizations, specifying how data will be exchanged in the Year 2000 and beyond, and developing contingency plans to ensure that core business functions can be performed even if systems fail. As further detailed in the following sections, while Defense is making good progress in renovating the legacy system and ensuring that the new system is compliant, it has not yet

²³Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

²⁴Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997). Published as an exposure draft in February 1997 and finalized in September 1997.

Adequate Interface Agreements
and Business Continuity and
Contingency Plans Not
Developed for Legacy System

ensured that its external interfaces will be remediated or developed effective contingency plans.

Defense has nearly completed renovation work on its legacy system, according to the Acquisition Program Manager, and release/deployment is planned for December 1998. In addition, in August 1998, Defense finalized a Year 2000 test plan for the legacy system. However, Defense does not yet have interface agreements that specify changes to date formats and how and when conflicts will be resolved with its data exchange partners.²⁵

Because noncompliant interfacing partners can introduce Year 2000-related errors into compliant systems, our Assessment Guide recommends that agreements with interface partners be established in the assessment phase in order to allow enough time for resolving conflicts. Until these agreements are in place, Defense will not have assurance that partners are working to correct interfaces effectively or promptly.

In addition, Defense has not developed adequate business continuity and contingency plans for the legacy system. To mitigate the risk that Year 2000-related problems will disrupt operations, our guide, entitled Year 2000 Business Continuity and Contingency Planning,²⁶ recommends that agencies perform risk assessments and develop and test realistic contingency plans to ensure the continuity of critical operations and business processes. Business continuity and contingency plans are important because they identify the manual or other fallback procedures to be employed should systems miss their Year 2000 deadline or fail unexpectedly in operation. Business continuity and contingency plans also define the specific conditions that will cause their activation.

In order for these plans to be effective, our guide recommends that, among other things, agencies analyze business process composition and priorities, dependencies, cycles, and service levels, and most important, the business process dependency on mission-critical information systems. The results of this analysis should be used to assess the cost and benefits of contingency alternatives and to identify and document contingency plans and implementation modes. These plans should define roles and responsibilities for contingency operations and provide a master schedule and milestones.

²⁵Defense has interface agreements for the legacy system that define general interface partner relationships and responsibilities, but these have not been updated to address these Year 2000 issues.

²⁶Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19). Published as an exposure draft in March 1998 and finalized in August 1998.

Defense recently developed a contingency plan for the legacy system, but this plan is perfunctory and does not meet the minimum criteria defined in our Business Continuity and Contingency Planning guidance which OMB has adopted as a standard for federal agencies. Specifically, the plan only states that if the legacy system fails, critical personnel actions will be prepared using one of three other commercial software packages. The plan does not provide a description of the resources, staff roles, procedures, and timetables needed for its implementation. And there is no evidence that Defense (1) assessed and documented risks posed by external systems and the public infrastructure, (2) defined the minimum acceptable level of outputs and services for each core business process, or (3) assessed the costs and benefits of contingency strategy alternatives.

The steps detailed in our guide are integral to helping agencies to manage the risk of potential Year 2000-induced disruptions to their operations. For example, the civilian personnel business area depends on information and data provided by other Defense and federal agencies whose systems can introduce Year 2000 problems into DCPDS. It also relies on services provided by the public infrastructure, which are susceptible to Year 2000 problems that could disrupt personnel operations—including power, water, and voice and data telecommunications. Until business continuity and contingency plans are developed that focus on this chain of critical dependencies, Defense will not be able to ensure that it can maintain the basic functionality of its core civilian personnel operations.

New System Facing Similar Risks

Since the new system already has a four-digit year field, it does not require renovation. Defense has obtained certification of Year 2000 compliance on all applications in the new system and completed Year 2000 tests on the system. However, CPMS has not identified all system interfaces or developed agreements with its interface partners. In addition, while CPMS recently developed a contingency plan, this plan is cursory. It only states that if the modern system fails, Defense will revert to using the legacy system for critical personnel actions. It is not based on a business impact analysis nor does it describe resources, staff roles, procedures, and timetables needed for its implementation.

As stressed above, even if the modernized system is compliant, Defense's civilian personnel management operations are at risk because of dependencies on external systems and the public infrastructure. Therefore, until it develops specific interface agreements and contingency plans that focus on critical dependencies, it will have no assurance that it can prevent Year 2000-related disruptions to critical personnel operations.

Conclusions

Because Defense did not consider alternatives, such as centralizing personnel functions, restructuring its regional and/or local offices to serve multiple agencies and services, or integrating payroll/personnel systems, its current regionalization approach may not be optimal. Defense lacked cost and performance data to analyze the options and it faced resistance from Defense components. While it may have required more time to develop needed data and greater management commitment to changing Defense business practices, the potential for substantially greater savings and efficiencies should have persuaded Defense to perform a rigorous analysis of all alternatives and to select the one proven most cost effective.

Additionally, because Defense did not adequately estimate and evaluate costs, benefits, and returns, there is not adequate assurance that its decision to replace the legacy system with the Oracle cots package is optimal. Furthermore, Defense does not know whether modifications to the Oracle product will satisfy its needs, how it will maintain the system, how it will protect sensitive data in the system, or how it will ensure the continuity of core civilian personnel operations in the event of Year 2000 failures. Despite this uncertainty, Defense reports having already spent about \$300 million on developing the system and establishing the regional offices and plans to spend hundreds of millions of dollars more to operate and support DCPDS and the regions.

Recommendations

Before Defense starts to deploy the new system beyond test sites, we recommend that the Secretary of Defense rigorously evaluate all business and system alternatives to providing personnel services as envisioned by the Clinger-Cohen Act, and, using this data and the system test results, select the most cost beneficial business and system alternative and develop and implement a transition plan for that alternative.

Specifically, business alternatives considered should include (1) use of regions and local offices to serve specific agencies or services, (2) use of regions or local offices to serve multiple agencies and services, (3) centralizing all or parts of personnel management operations that currently operate at component headquarters and major commands, (4) integrating DOD's civilian personnel and payroll management systems, (5) outsourcing civilian personnel computer operations, (6) outsourcing all civilian personnel management services, and (7) acquiring other commercially available products. In analyzing commercially available products, we recommend that Defense consider the costs, benefits, and returns-on-investment of all commercially available products that support

personnel management. We also recommend that the analysis of commercially available products consider technical risks, including whether each available product can support Defense's needs and whether each one can be modified in the future at a reasonable cost. In evaluating the range of business alternatives consideration should be given to the substantial investment that has already been made in the current approach.

Regardless of the business and system alternative selected, we recommend that Defense optimize it by collecting, analyzing and using reliable cost and performance data and making improvements. We also recommend that, regardless of the chosen approach, Defense take the following actions to mitigate technical, security, and Year 2000 risks.

- To ensure that the system is adequately maintained and that modifications are carefully controlled, Defense should (1) develop agreements with system partners and interface partners to define responsibility for system operations, maintenance, and security, (2) establish a configuration control board comprised of system users to assist in deciding on which changes need to be made to the system, prioritizing change requests, and ensuring that changes are correctly made, (3) assign clear responsibility for providing technical assistance to Defense components.
- To ensure that sensitive personnel data are adequately protected, Defense should (1) assess its risks and determine security needs, (2) define and implement appropriate policies and related controls, including standards for encrypting data and firewalls, (3) promote security awareness at all sites maintaining the system, and (4) continually monitor and evaluate policy and control effectiveness.
- To mitigate Year 2000 risks, Defense should (1) establish interface agreements that clearly specify date format changes, time frames for these changes, and processes for resolving conflicts, (2) refine business continuity and contingency plans to ensure that they consider risks posed by external systems and infrastructure; assess the costs and benefits of alternative contingency strategies; and describe resources, staff roles, procedures, and timetables needed for implementation of the plan, and (3) test contingency plans to ensure that they are capable of providing the desired level of support to the agency's core business processes and can be implemented within a specified period of time.

Agency Comments and Our Evaluation

The Acting Assistant Secretary for Force Management Policy provided written comments on a draft of this report, which are reprinted in

appendix I. He concurred with all five of our recommendations and agreed to evaluate recommended alternatives as Defense proceeds with its regionalization and modernization efforts.

In concurring with our recommendations, however, Defense questioned our use of the Clinger-Cohen Act of 1996 as criteria for evaluating civilian personnel system decisions since these decisions were made before the act took effect. We used the Clinger-Cohen Act to evaluate Defense's decisions because the act's requirements reflect basic and widely accepted principles of sound system acquisition management. Similar practices are also called for in OMB Circulars A-11 and A-130, the Chief Financial Officers Act of 1990, the Government Performance and Results Act of 1993, the Federal Acquisition Streamlining Act of 1994, and the Paperwork Reduction Act of 1995—all of which were applicable in some manner to Defense's decisions in this effort. Moreover, Defense was required to follow such practices by its own system acquisition regulations and guidelines. Finally, during the course of our review, Defense officials responsible for DCPDS told us that they were attempting to follow Clinger-Cohen Act principles in developing the system. Appendix I provides our detailed responses to Defense's views on our recommendations and findings.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Armed Services; Senate Committee on Governmental Affairs; Subcommittee on Defense, Senate Committee on Appropriations; House Committee on Armed Services; Subcommittee on Defense, House Committee on Appropriations; and Senate and House Committees on the Budget; the Secretary of Defense; the Senior Civilian Official of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence; the Under Secretary of Defense (Comptroller); the Acting Assistant Secretary of Defense for Force Management Policy; and the Director, Office of Management and Budget. Copies will also be made available to others upon request.

If you have any questions about this report, please call me or Carl Urie, Assistant Director at (202) 512-6240. Other major contributors of this report are listed in appendix III.

A handwritten signature in black ink, appearing to read 'J. Brock, Jr.', with a stylized, cursive script.

Jack L. Brock, Jr.
Director, Governmentwide and Defense
Information Systems

Contents

Letter	1
Appendix I Comments From the Department of Defense	32
Appendix II Scope and Methodology	44
Appendix III Major Contributors to This Report	47
Tables	
Table 1: Differences in Personnel Management	7
Table 2: Estimated Costs of Defense's Personnel Initiative	10

Contents

Abbreviations

AFB	Air Force Base
AFOTEC	Air Force Operational Test and Evaluation Center
CDA	Central Design Activity
COTS	commercial-off-the-shelf
CFO	chief financial officer
CPMS	Civilian Personnel Management Service
DCPDS	Defense Civilian Personnel Data System
DISA	Defense Information Systems Agency
DOD	Department of Defense
FASA	Federal Acquisition Streamlining Act of 1994
GPRA	Government Performance and Results Act of 1993
I-CASE	Integrated Computer-Aided Software Engineering
IDIQ	indefinite delivery, indefinite quantity
IT	information technology
MAISRC	Major Automated System Review Council
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
PA&E	Program Analysis and Evaluation
PRA	Paperwork Reduction Act of 1995
USDA	Department of Agriculture

Comments From the Department of Defense

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



FORCE MANAGEMENT
POLICY

ASSISTANT SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

JAN 11 1999



Mr. Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Dodaro:

This is the Department of Defense (DoD) response to the General Accounting Office (GAO) draft report, "DEFENSE IRM: Alternatives Should Be Considered in Developing the New Civilian Personnel System," dated November 25, 1998 (GAO Code 511634/ OSD Case 1719).

DoD agrees with the report's findings that: regionalization of civilian personnel service delivery and the modernization of the Defense Civilian Personnel Data System (DCPDS) can potentially improve civilian personnel operations and achieve cost savings; we have eliminated a number of personnel management information systems that were redundant and not interoperable; we have made good progress in renovating the legacy DCPDS and ensuring the modern system's compliance with the Year 2000 computing demands; and we have improved processes for developing, tracking, and monitoring personnel actions, handling injury compensation claims, and estimating retirement eligibility benefits.

DoD agrees with the recommendation to consider business alternatives in addition to the current approach and to include commercially available products in its ongoing analysis of system alternatives. DoD regards the current regionalization and systems modernization initiative as part of a continuing and evolutionary improvement program. Therefore, we will consider recommended alternatives as we continue our regionalization and systems modernization efforts.

The report notes that DoD did not apply some requirements (e.g., Clinger-Cohen Act, OMB Circulars A-11, A-130) in deciding to develop the modern DCPDS. However, these requirements did not exist when DoD made the decision. The Department supports the goals of the Clinger-Cohen Act and strives to balance sound objective data with business-based decisions reflecting real-world experience. We believe the initial estimates of costs, benefits, and returns were adequate to assure that the concept of regionalizing civilian personnel service delivery and modernizing the supporting information system would provide substantial cost savings.

The Department has made a significant commitment to improving the operations of its civilian personnel function. It should be noted that the modern DCPDS was under development

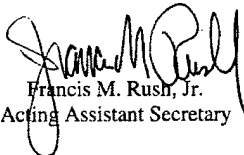


See comment 1.

Appendix I
Comments From the Department of Defense

during the period of the GAO review and is now in the final testing stages. Additional comments are provided in the enclosure to this letter.

Sincerely,


Francis M. Rush, Jr.
Acting Assistant Secretary

Enclosure:
DoD Response

**GAO DRAFT REPORT – DATED NOVEMBER 25, 1998
GAO CODE 511634/OSD CASE 1719**

**“DEFENSE IRM: ALTERNATIVES SHOULD BE CONSIDERED IN DEVELOPING
THE NEW CIVILIAN PERSONNEL SYSTEM”**

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

The Department of Defense (DoD) has approached civilian personnel regionalization and systems modernization in a rational, logical, and systematic manner despite the dramatic changes that have influenced these major initiatives since their inception. While there is no doubt that following many of the GAO recommendations could have been beneficial, the Department was under pressure to seize opportunities to respond to base closures, workforce reductions, and streamlining initiatives.

To meet these challenges, the Department's civilian personnel community recognized early that economies and efficiencies could be achieved only by undertaking aggressive action to change the fundamental way DoD delivered civilian personnel services. This strategy included:

- Streamlining civilian personnel management by consolidating and simplifying policies and procedures within a common regulatory framework.
- Consolidating, streamlining, and standardizing common staff functions and services to reduce unnecessary overhead and achieve economies of scale.
- Developing and implementing a standard civilian personnel management information system with improved performance and reduced costs.
- Reducing the size of installation-level civilian personnel offices by centralizing the majority of services performed.

DoD considers the current regionalization and systems modernization initiative as part of a continuing and evolutionary improvement program. Because we believe that further changes of this magnitude need to be pursued, as GAO proposes, with fact-based analysis, we are taking a series of steps to obtain more precise data on regionalization and modernization costs and associated benefits. The differing Component approaches to regionalization will allow us to consider best practices carefully for future improvements to the program.

While the Department may not have conducted the cost and performance data analysis envisioned in the GAO report, there were sufficient data available to indicate that civilian personnel servicing ratios (labor costs) could be improved significantly through economies of scale. The data clearly showed that larger DoD personnel offices achieved higher servicing ratios by having a larger customer base, by concentrating the service providers, by performing volume processing of actions, by standardizing processes, and by using technology. The civilian personnel community recognized that change of this magnitude would best be achieved through incremental improvements that would strike a balance between the rate of transition and the

See comment 2.

See comment 1.

ability of DoD Components to absorb the changes without risking any impairment of timely and quality service to its managers and employees.

The report notes that DoD did not apply some requirements (e.g., 1996 Clinger-Cohen Act, OMB Circulars A-11, A-130) in deciding to develop the modern DCPDS. However, these requirements did not exist when the decisions were being made. As our actions since then indicate, we support the goals of the Clinger-Cohen Act and strive to balance sound objective data with business based decisions reflecting real-world experience. We believe that the initial estimates of costs, benefits, and returns were adequate to assure that the concept of regionalizing civilian personnel service delivery and modernizing the supporting information system would provide substantial cost savings. From its beginning the DCPDS modernization program, has received continuous and intense oversight from the DoD Major Automated Information Systems Review Council (now called the Overarching Integrated Product Team). We have rigorously followed the joint analytical process laid out by this group.

The Department also notes that at the time the decision was made to build the modern DCPDS, very few commercial human resources management systems were available besides the three products that were evaluated. Based on the review of these products, and the data that were in hand, we believe the benefits of fielding the modern DCPDS to DoD Components will significantly exceed its costs. Nonetheless, the Department is taking a series of steps to obtain more precise data on regionalization and modernization costs and associated benefits. This effort will lay the foundation for examining the other alternatives recommended in the GAO report. Any changes, however, will continue to be made as evolutionary improvements, and will be approached from the standpoint of the Department's ability to maintain critical capabilities while making the changes.

TECHNICAL CORRECTION:

In responding to the first question ("In developing, managing and overseeing DCPDS, is Defense applying the Clinger-Cohen Act?") the draft GAO report discusses the scoring of the software products reviewed and provides the weights of the scoring criteria. Because this information was part of the procurement process, it should not be addressed in a public document. Identification of the scoring criteria could jeopardize future procurements. We therefore request that this scoring information be removed from the report.

RECOMMENDATIONS:

RECOMMENDATION 1: GAO recommends that the Secretary of Defense rigorously evaluate all business and system alternatives to providing personnel services as envisioned by the Clinger-Cohen Act, before starting to deploy the new system beyond test sites, and, using these data and system test results, select the most cost-beneficial business and system alternative and develop and implement a transition plan for that alternative. (p. 42/GAO Draft Report)

DOD RESPONSE: Concur. We will evaluate business and system alternatives, select the most cost-beneficial, and implement a transition plan for this alternative prior to deployment beyond

See comment 3.

Appendix I
Comments From the Department of Defense

the test sites. The Department has always agreed with the principle of continuous evaluation of alternatives, seeking new solutions, and applying cost-benefit analysis. The Department has never viewed this program as an end state, but rather as a basis for further evolutionary improvements in civilian personnel systems and service delivery.

As of the end of FY 1998, an estimated reduction of over 1,500 human resources (HR) specialists (out of a total reduction of almost 3,900) can be attributed to the program. This represents cost avoidance of over \$100M annually. When savings from streamlined systems operations are included, the program has already repaid its investment to date (see enclosed September 1998 Regionalization and Systems Modernization Economic Analysis).

The Department has demonstrated steady progress in attaining its HR servicing ratio goal, with an improvement from 1:67 to 1:77 since FY 1994 (almost twice the reduction rate for HR specialists as for the Department's general population). The Department will continue to reduce the number of HR specialists, providing an estimated savings of \$1.5B over this program's life cycle. The remaining investment in the program to field the modern system and complete regionalization is required to sustain this aggressive reduction pace and realize the savings already incorporated in out-year budgets.

The Department has actively pursued the alternatives provided with this recommendation. Specifically:

- By allowing the Military Departments and Defense agencies to establish different servicing options, we will be able to evaluate both internal servicing and cross-servicing in the regional environment. We will continue to evaluate the regionalization concept and share efficiencies across Component lines as suggested in business alternatives (1) and (2).
- Business alternative (3) was partially implemented by Defense Management Report Decision (DMRD) 974, Civilian Personnel Administration Efficiencies (1991 and 1992). As a result, we deregulated civilian personnel by unifying and simplifying policies and consolidated, in the Civilian Personnel Management Service, common staff functions formerly performed at Component headquarters and major commands. This consolidation resulted in a 23 percent reduction in personnel performing these functions. We will continue to look for efficiencies by studying the possibility of consolidating additional Component-level programs.
- With regard to business alternative (4), the OSD PA&E "Civilian Personnel/Payroll Cost Analysis," September 1994, examined several in-house and outsourcing options for personnel and payroll services. It concluded that an in-house personnel service in a regionalized environment with a modernized DCPDS was the most cost-effective alternative. [Copy attached] The Department is also currently looking at conducting an A-76 study on the performance of civilian pay operations, and the results of that study will affect the technical solutions pursued in the future.
- The Department is already working on business alternatives (5) and (6). First, review of civilian personnel operations is included in the Department's current Review of Inherently

See comment 4.

See comment 5.

Appendix I
Comments From the Department of Defense

Governmental Functions (Department of Defense Reform Initiative # 20). The Components are conducting a rigorous exercise to review positions to identify potential outsourcing opportunities. One Component is working to query the market place. This is being done through a Sources Sought Synopsis which will include notice to the Commerce Business Daily asking vendors capable of performing the advertised functions to identify their interest. Additionally, we are actively considering the option of a performance-based outsourcing effort for the operation, sustainment, and future enhancement of the modern DCPDS.

- We have always supported the principle recommended in alternative (7) to evaluate of systems alternatives continuously. After the modern DCPDS is fielded and stabilized, we will continue to look at the available commercial software for future enhancements. DoD will consider the costs, benefits, and return-on-investment following the principles recommended by GAO for future systems development efforts.

RECOMMENDATION 2: Regardless of the business and system alternative selected, GAO recommends that Defense help optimize it by collecting, analyzing and using reliable cost and performance data. (p. 43/GAO Draft Report)

DOD RESPONSE: Concur. Several of the Components have developed comprehensive metrics systems for measuring the timeliness and volume of Regional Service Center (RSC) work that they use as a tool to manage RSC operations and resources. DoD will use these data, and will build upon them, to assess and improve the entire regionalization effort within the Department.

RECOMMENDATION 3: To ensure that the system is adequately maintained and that modifications are carefully controlled, GAO recommends that Defense should (1) develop agreements with system partners and interface partners to define responsibility for system operations, maintenance, and security, (2) establish a configuration control board comprised of system users to assist in deciding on which changes need to be made to the system, prioritizing change requests, and ensuring changes are correctly made, (3) assign clear responsibility for providing technical assistance to Defense components. (p. 43/GAO Draft Report)

DOD RESPONSE: Concur. Actions are underway to ensure that the modern DCPDS is adequately maintained and that modifications are carefully controlled. Recommended actions (1), (2), and (3) will be completed once the decision is made to use a government or commercial source to operate, maintain, and modify the modern DCPDS.

DoD hired a contractor to research the possibility of outsourcing the operation and maintenance of the modern DCPDS. The report provided recommendations on how the system should be managed and operated. Based upon the findings, *A Concept of Operations Plan for the Maintenance, Sustainment and Operation of the Modern Defense Civilian Personnel Data System*, dated December 9, 1997, which outlines responsibilities, was provided to Components. We will continue to work on refining draft documents which provide a performance-based statement of work, a matrix establishing detailed roles and responsibilities, service-level requirements and performance measures, and the technical evaluation criteria for modern

See comment 6.

Appendix I
Comments From the Department of Defense

DCPDS operations. These documents address help desk support, database administration, systems administration, application sustainment and maintenance, transition planning and implementation, and technology refresh.

Listed below are timelines required to establish either a government or commercial service-provider solution.

Government Decision:

Identify Potential Providers	+ 30 Days
Develop Agreements with System Partners	+ 45 Days
Establish Configuration Control Board	+ 45 Days
Review Capabilities	+ 75 Days
Negotiate Interservice Support Agreements	+ 95 Days
Transition	+180 Days

Commercial Decision:

Complete Statement of Work	+ 45 Days
Issue Request for Proposals	+ 45 Days
Develop Agreements with System Partners	+ 45 Days
Establish Configuration Control Board	+ 45 Days
Review Vendor Proposals	+105 Days
Perform Technical Evaluation	+185 Days
Contract Award	+195 Days
Transition	+280 Days

RECOMMENDATION 4: To ensure that sensitive personnel data are adequately protected, GAO recommends that Defense should (1) assess its risks and determine security needs, (2) define and implement appropriate policies and related controls, including standards for encrypting data and firewalls, (3) promote security awareness at all sites maintaining the system, and (4) continually monitor and evaluate policy and control effectiveness. (Pp. 43-44/GAO Draft Report)

See comment 7.

DOD RESPONSE: Concur. We agree that in any systems development effort the program management staff must assess risk and determine the system level security needs. This has been accomplished. An initial risk assessment of the modern DCPDS performed in December 1995 identified potential vulnerabilities that could pose a security risk for the modern DCPDS. The modern DCPDS Computer Security Work Group (CSWG)¹ performed a risk analysis² in October 1997, taking a critical look at the modern DCPDS as well as the operational environment. A Security Test and Evaluation (ST&E)³ of the modern DCPDS was accomplished in the fall of

¹ The DCPDS CSWG is a Component level working group chaired by the Civilian Personnel Management Service with membership from the CDA (Central Design Activity) and each Component to be supported by the DCPDS modern system.

² Defense Information Systems Agency (DISA) MAISRC representatives facilitated the risk assessment.

³ Overseen by an Independent Verification and Validation team appointed by DISA MAISRC.

1998, at the Central Design Activity (CDA). The review will be formally completed in early 1999. The ST&E evaluated the modern DCPDS technical security features implemented in support of the modern DCPDS Security Policy. Most recently, the Air Force Information Warfare Center performed a Computer Security Engineering Assessment during September and October 1998. These formal and informal risk assessments were used to identify potential vulnerabilities and weaknesses that could be exploited. The ST&E and Computer Security Engineering assessments were used to evaluate the technical and operational security features implemented in response to the identified vulnerabilities and weaknesses, as well as the security principles espoused in the modern DCPDS Security Policy. Additionally, a Security Features User's Guide, a Security Annex to the Training Support Plan, and a four-volume set of Trusted Facility Manuals have been developed to support security awareness and training. As the modern DCPDS is being fielded, the individual Components will accomplish a risk analysis at each of their operational locations to evaluate the operational implementation of the security guidance provided by the design activity.

We agree that encryption of sensitive but unclassified data transmitted over the DISA-managed Non-secure Internet Protocol Router Network (NIPRNet) is prudent. CPMS is procuring a package to encrypt DCPDS data at Initial Operating Capability. Advanced Networking Options (ANO), an Oracle proprietary encryption solution, will be used to satisfy our functional requirement for data privacy during transmission between customer support units and supervisors at the installation level, regional service centers, and a corporate-level data warehouse. This product is being tested at the CDA. This encryption solution, combined with individual Component firewall policies, will provide protection of the sensitive unclassified DCPDS data.

Within the modern DCPDS environment, each operational location will have an Information System Security Officer (ISSO) or system manager who will be responsible to the local Designated Approving Authority (DAA) for ensuring the secure operation of the modern DCPDS. Combined with remote system administration, staff assistance visits, and periodic reaccreditation, this will ensure that the technical and operational security measures are implemented.

RECOMMENDATION 5: To mitigate Year 2000 risks, GAO recommends that Defense should (1) establish interface agreements that clearly specify date format changes, timeframes for these changes, and processes for resolving conflicts, (2) refine business continuity and contingency plans to ensure that they consider risks posed by external systems and infrastructure; assess the costs and benefits of alternative contingency strategies; and describe resources, staff roles, procedures, and timetables needed for implementation of the plan, and (3) test contingency plans to ensure that they are capable of providing the desired level of support to the agency's core business processes and can be implemented within a specified period of time. (p. 44/GAO Draft Report)

DOD RESPONSE: **Concur.** CPMS currently has interface agreements with the owners of our major external interfaces, many of which do not require date changes. However, we will work with our partners to review and update existing interface agreements and ensure the agreements support the exchange of data between those systems. We will ensure the agreements clearly

See comment 8.

Appendix I
Comments From the Department of Defense

See comment 9.

describe any applicable date format changes and timelines for when those changes must be accomplished and comply with the "Year 2000 Management Plan" draft published in June of this year. We will also ensure that an adequate process is in place to resolve any conflicts that might arise due to these changes. These actions are planned for completion by April 1999.

CPMS issued a Contingency Management Manual, which provides a set of guidelines, a common set of terms, and a description of the basic division of responsibilities for performing contingency management tasks. Components used this manual to prepare their contingency plans. In addition, a Y2K contingency plan to assist in the Components' development of local continuity and contingency plans has been prepared. We will continue to work with the Components to refine this contingency plan to ensure that the DoD guidance is adequate for Component organizations to develop robust, realistic contingency plans. CPMS and the Components plan to complete these tasks by May 1999.

See comment 9.

As part of its responsibility for overseeing contingency plans, CPMS will ensure that Component plans include requirements to test the specific contingency processes of the chosen alternative. Testing will include processing real-time personnel actions in the manual mode, delivery of these actions to the appropriate payroll office, preparation of required support documents, and recovery of actions in the automated database after completion (to ensure duplicate actions are not processed at payroll). We estimate the time to begin initial testing of continuity and contingency is June 1999. This timeline will allow for additional testing prior to January 2000.

Enclosures:

September 1998 Reg/Mod Economic Analysis

September 1994 PA&E Civilian Personnel/Payroll Cost Analysis

The following are GAO's comments on the Department of Defense's letter dated January 11, 1999.

GAO Comments

1. Although the Clinger-Cohen Act was not in existence when DOD made the initial decisions in developing the modern DCPDS, it has been in effect since 1996 and should have been applied to all decisions made subsequent to its enactment. Further, OMB Circulars A-11 and A-130 existed prior to the initial decisions related to DCPDS and included basic principles of sound system acquisition management. In addition, several acts that were in effect when the initial decisions were made contain requirements similar to those outlined in the Clinger-Cohen Act relating to improved information technology management in the federal government. For example (1) the Government Performance and Results Act of 1993 (GPRA) requires federal agencies to set strategic goals, measure performance, and report on accomplishments, (2) the Federal Acquisition Streamlining Act of 1994 (FASA), Title V, requires agencies to define cost, schedule, and performance goals for federal acquisition programs (including information technology projects) and to monitor these projects to ensure that they remain within prescribed tolerances, (3) the Paperwork Reduction Act of 1995 (PRA) emphasizes achieving program benefits and meeting agency goals through the effective use of information technology, and (4) the Chief Financial Officers (CFO) Act of 1990 focuses on the need to improve financial management and reporting practices of the federal government, which is critical for knowing an information technology project's actual costs and for computing accurate returns on investment. Finally, Defense's own system acquisition regulations and guidelines, in existence at the time Defense made the initial decisions in developing the modern DCPDS, include requirements similar to those outlined in the Clinger-Cohen Act related to basic principles of sound system acquisition management.

2. Before embarking on an improvement approach for its civilian personnel mission area, Defense performed cost and performance analyses which indicated the Department's civilian personnel servicing ratios could be improved significantly. However, because these analyses did not fully consider the costs and benefits of numerous alternative business and systems approaches for improving the servicing ratios, the Department may not have selected the most cost-effective improvement approach.

3. We revised the report to delete specific information on the scoring criteria used in the DCPDS procurement.

4. While Defense reports that it has already consolidated some civilian personnel functions at component headquarters and major commands and reduced staff by 23 percent, in June of 1998, there were still 886 people performing civilian personnel management and oversight functions at component headquarters and major command levels at a cost of about \$63 million a year. Given that the Civilian Personnel Management Service performs the same management and oversight functions as component headquarters and major commands, there are substantial opportunities for further consolidation and staff reduction.

5. The A-76 study includes some but not all promising alternatives. While it will evaluate outsourcing civilian pay operations, it will not consider outsourcing personnel operations or integrating personnel and payroll systems. Furthermore, while Defense considered the possibility of outsourcing personnel computer operations in 1994, it lacked the cost and performance data necessary to sufficiently analyze this approach.

6. While it is important for Defense components to develop comprehensive metrics to measure the timeliness and value of regional service center work, they must also standardize these metrics so that meaningful comparisons can be made across the Department. The components must also collect baseline data that define the current operations so that Defense can determine whether new systems and business strategies are achieving predicted cost and performance improvements.

7. If implemented effectively, the site-by-site risk assessments and other actions Defense is taking should help address the security concerns identified in this report. However, to maximize protection over DCPDS data, Defense still needs to establish departmentwide standards on encryption and firewalls.

8. Although CPMS has interface agreements with the owners of major external interfaces for the legacy DCPDS system, those agreements have not been adequately updated to include Year 2000 issues. Specifically, the agreements do not define agreed upon date formats, nor describe how problems with data exchanges will be resolved. Further, as of the completion of our review, CPMS had not identified the system interfaces or developed agreements with its interface partners for the modern DCPDS.

9. Defense plans to complete interface agreements by April 1999 and contingency plans by May 1999 and to begin testing contingency plans by June 1999. However, the Office of Management and Budget and GAO's Year

Appendix I
Comments From the Department of Defense

2000 guidance recommend that agencies develop interface agreements and realistic contingency plans during the assessment phase, i.e., by August 1997, in order to minimize the risk of Year 2000 problems.

Scope and Methodology

To analyze how Defense determined the number and locations for civilian personnel regional service centers and why there is a wide disparity in the number of regional centers among the services, we interviewed Office of the Secretary of Defense, military service, and Defense agency officials and reviewed guidance mandating regionalization, the services' and Defense agencies' regionalization studies, and their rationale for determining the number and location of regions. Where appropriate, we interviewed officials from CPMS, the military services, and the Washington Headquarters Service to understand perspectives regarding regionalization plans and status of regionalization actions. We visited five regional centers, toured the facilities, and interviewed numerous officials. These five centers were Ft. Riley, Kansas; Aberdeen Proving Ground, Maryland; Silverdale, Washington; Randolph AFB, Texas; and Washington, D.C.

To assess whether Defense is applying the Clinger-Cohen Act in overseeing, managing, and developing DCPDS, we compared Defense's actions taken on DCPDS to the investment principles included in the act. We reviewed GAO, OMB,¹ and Defense best practices guidance² for implementing the Clinger-Cohen Act and reviewed other Defense policies and guidance for developing and implementing information systems. We analyzed selected major studies of information technology and personnel management matters in Defense, including studies by Coopers & Lybrand, a consulting organization³ and the Defense Science Board,⁴ prior GAO studies of major defense information systems projects, and selected Defense Office of Inspector General reports. We interviewed appropriate Defense and OMB representatives familiar with personnel legislative requirements and officials responsible for the development and oversight of DCPDS, including officials from CPMS, the Major Automated Information System Review Council (MAISRC), the Under Secretary of Defense/Comptroller, the Comptroller's Program Analysis and Evaluation (PA&E) unit, and service and agency staff responsible for regionalization, and DCPDS program management.

¹Office of Management and Budget, Capital Programming Guide, Version 1.0, Supplement to Office of Management and Budget Circular A-11, Part 3: Planning, Budgeting, and Acquisition of Capital, July 1997.

²Department of Defense Software Acquisition Best Practices Initiative, The Program Manager's Guide to Software Acquisition Practices, undated.

³Department of Defense, Office of the Comptroller, Civilian Personnel/Payroll Private Sector Benchmarking Survey, Final Report, Coopers & Lybrand, September 21, 1994.

⁴Defense Science Board, Report of the Defense Science Task Force: Military Personnel Information Management, August 31, 1996.

To determine whether DCPDS duplicates the Employee Express System available through the Office of Personnel Management (OPM), we reviewed documentation Defense prepared justifying the need for DCPDS and Defense documentation reviewing the Employee Express System. We requested that OPM review and comment on Defense's rationale for not using the Employee Express system; we requested that Defense respond to OPM's comments; and we analyzed both Defense's and OPM's positions on this issue. In addition, we contacted representatives of six other federal organizations that were developing new civilian personnel systems and were not using the Employee Express system to determine their rationale.

To determine whether (1) Defense's civilian personnel management requirements are sufficiently different to require extensive modification of the commercial-off-the-shelf software (COTS) application which Defense selected as the foundation for developing DCPDS and (2) Defense leadership was aware of the extent and cost of modifications that would be needed, we interviewed the Functional and Acquisition Program managers and their staff as well as representatives of the Oracle Corporation to solicit information on the selection, acquisition, and modification of the Oracle COTS product.

To assess whether Defense identified and mitigated the risks associated with the major modifications, we interviewed CDA officials to determine Defense's actions to date, including those planned, in process, and completed to address mitigating risks in overseeing, managing, and developing DCPDS. We reviewed pertinent regulations, studies, and documentation, including the technical risk analysis, configuration management plan, testing plans, and the Department's Program Manager's Guide to Software Acquisition Best Practices. As requested, we determined whether Defense used this guide in overseeing, managing, and developing DCPDS. In assessing security risks, we reviewed Defense's Deployment, Concept of Operations, Encryption, Security Support, and Contingency Plans. We reviewed Defense directives and regulations on computer security, including Regulation 5000.2-R, dated March 23, 1998, Directive 5200.28, dated March 21, 1998, and Military Standard 498, dated December 1994. In addition, we assessed the physical security threats at four local and four regional offices, through interviews and observations. In assessing Year 2000 risks, we reviewed the Year 2000 plans for the legacy and modern systems and we compared these plans to our own Year 2000 Assessment Guide.⁵ We conducted our review from August 1997

⁵Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14). Issued as an exposure draft in February 1997 and finalized in September 1997.

Appendix II
Scope and Methodology

through July 1998 in accordance with generally accepted government auditing standards.

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

Dr. Rona Stillman, Chief Scientist
Carl M. Urie, Assistant Director
Brian C. Spencer, Technical Assistant Director
Cristina T. Chaplain, Communications Analyst
Robert L. Crocker, Jr., Senior Evaluator

Kansas City Field Office

George L. Jones, Evaluator-in-Charge
David R. Solenberger, Senior Evaluator
Denise M. Wempe, Senior Evaluator
Karl G. Neybert, Staff Evaluator

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

<http://www.gao.gov>